日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出　願　年　月　日
Date of Application:　２００３年　７月２５日

出　願　番　号
Application Number:　特願２００３－２０２００４

[ST. 10/C]:　［ＪＰ２００３－２０２００４］

出　願　人
Applicant(s):　東北大学長

２００３年１２月　５日

特許庁長官
Commissioner,
Japan Patent Office　今井康夫

出証番号　出証特２００３－３１００６９１

【書類名】　特許願
【整理番号】　U2003P078
【特記事項】　特許法第３０条第１項の規定の適用を受けようとする特許出願
【提出日】　平成15年 7月25日
【あて先】　特許庁長官　今井　康夫　殿
【国際特許分類】　G09C　5/00
【発明の名称】　音像定位を活用した音響秘密情報分散装置、その方法およびプログラム
【請求項の数】　15
【発明者】
【住所又は居所】　宮城県仙台市青葉区上杉５－８－７０－６０６
【氏名】　静谷　啓樹
【発明者】
【住所又は居所】　宮城県仙台市青葉区川内　東北大学情報シナジーセンター情報教育研究部内
【氏名】　満保　雅浩
【特許出願人】
【識別番号】　391012394
【氏名又は名称】　東北大学長　吉本　高志
【代理人】
【識別番号】　100072051
【弁理士】
【氏名又は名称】　杉村　興作
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9711018

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　音像定位を活用した音響秘密情報分散装置、その方法およびプログラム

【特許請求の範囲】

【請求項１】　音像定位を活用した音響秘密情報分散装置であって、

秘密情報として少なくとも１つのターゲット音を複数のステレオメディアに分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央からずれるように分散する第1の信号処理器と、

攪乱情報として複数のデコイ音を前記複数のステレオメディアにそれぞれ分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央に定位するように分散する第２の信号処理器と、

を含むことを特徴とする音響秘密情報分散装置。

【請求項２】　請求項１に記載の音響秘密情報分散装置において、

前記第1の信号処理器および前記第2の信号処理器は、

前記ステレオメディアの左右のチャンネルの音量を調整することによって、前記音像が頭部中央からずれるか否かを制御している、

ことを特徴とする音響秘密情報分散装置。

【請求項３】　請求項１または２に記載の音響秘密情報分散装置において、

前記ターゲット音の数と前記デコイ音の数との和ｎは、６以下である、

ことを特徴とする音響秘密情報分散装置。

【請求項４】　請求項１～３のいずれか1項に記載の音響秘密情報分散装置において、

前記ステレオメディアにおける１つの音信号の片側の最大振幅ｐは、ほぼ１０以下である、

ことを特徴とする音響秘密情報分散装置。

【請求項５】　請求項１～４のいずれか1項に記載の音響秘密情報分散装置において、

所望の安全率、および／または、想定される結託者率に基づき、前記ステレオメディア数を算出する計算手段、

をも含むことを特徴とする音響秘密情報分散装置。

【請求項６】　音像定位を活用した音響秘密情報分散方法であって、

秘密情報として少なくとも１つのターゲット音を複数のステレオメディアに分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央からずれるように分散する第1のステップと、

攪乱情報として複数のデコイ音を前記複数のステレオメディアにそれぞれ分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央に定位するように分散する第２のステップと、

を含むことを特徴とする音響秘密情報分散方法。

【請求項７】　請求項６に記載の音響秘密情報分散方法において、

前記第1および前記第2のステップは、

前記ステレオメディアの左右のチャンネルの音量を調整することによって、前記音像が頭部中央からずれるか否かを制御している、

ことを特徴とする音響秘密情報分散方法。

【請求項８】　請求項６または７に記載の音響秘密情報分散方法において、

前記ターゲット音の数と前記デコイ音の数との和ｎは、６以下である、

ことを特徴とする音響秘密情報分散方法。

【請求項９】　請求項５～８のいずれか1項に記載の音響秘密情報分散方法において、

前記ステレオメディアにおける１つの音信号の片側の最大振幅ｐは、ほぼ１０以下である、

ことを特徴とする音響秘密情報分散方法。

【請求項１０】　請求項５～９のいずれか1項に記載の音響秘密情報分散方法において、

所望の安全率、および／または、想定される結託者率に基づき、演算手段を用いて前記ステレオメディア数を算出する計算ステップ、

をも含むことを特徴とする音響秘密情報分散方法。

【請求項１１】　音像定位を活用した音響秘密情報分散方法をコンピュータに実行させるためのプログラムであって、

前記方法は、
秘密情報として少なくとも１つのターゲット音を複数のステレオメディアに分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央からずれるように分散する第1のステップと、
攪乱情報として複数のデコイ音を前記複数のステレオメディアにそれぞれ分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央に定位するように分散する第２のステップとを含む
ことを特徴とするプログラム。
【請求項１２】　請求項１１に記載のプログラムにおいて、
前記第1および前記第2のステップは、
前記ステレオメディアの左右のチャンネルの音量を調整することによって、前記音像が頭部中央からずれるか否かを制御している、
ことを特徴とするプログラム。
【請求項１３】　請求項１１または１２に記載のプログラムにおいて、
前記ターゲット音の数と前記デコイ音の数との和ｎは、６以下である、
ことを特徴とするプログラム。
【請求項１４】　請求項１１～１３のいずれか１項に記載のプログラムにおいて、
前記ステレオメディアにおける１つの音信号の片側の最大振幅ｐは、ほぼ１０以下である、
ことを特徴とするプログラム。
【請求項１５】　請求項１１～１４のいずれか１項に記載のプログラムにおいて、
所望の安全率、および／または、想定される結託者率に基づき、演算手段を用いて前記ステレオメディア数を算出する計算ステップ、
をも含むことを特徴とするプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】

本発明は、音像定位を活用した音響秘密情報分散方式、その方法およびプログラムに関するものである。

【０００２】

【従来の技術】

秘密情報の安全かつ柔軟な管理や知的所有権の保護リスク管理などを実現するために、テジタル情報を分散管理する秘密分散手法の研究が盛んである（非特許文献１、２および３を参照されたい。）。また、近年では、画像情報の分散手法である視覚秘密分散手法の研究も行なわれており、（非特許文献４および５を参照されたい。）、視覚特性を利用することにより、秘密情報である画像の復号に特別な装置を必要としない手法が開発されている。これは、例えば、各々を見ただけでは何が写っているのかわからない2枚の画像を重ね合わせて見ることによって、１つの意味のある画像を浮かび上がらせるという手法である。

そして、視覚秘密分散手法と同様に、復号に特別な装置を必要としない手法を音響に適用する技術も提案されている。しかしそのような特性を有する音響秘密分散手法はデスメット他が提案する「非バイナリ音声暗号化」（非特許文献６を参照されたい。）のみである。しかし、この手法では、分散情報の生成に複雑な信号処理（例えば離散フーリエ変換など）が必要であり不便であるため、この手間を省く手法を考案できれば、音楽関連の会社など多量の音響情報を分散する機関にとって有益となる。

秘密分散手法とは異なるが、聴覚特性を利用した情報セキュリティシステムとして、電子透かし手法が、富岡他による「マルチチャンネルディジタルオーディオに対する電子透かし」（非特許文献７を参照されたい。）で提案されている。これは、マルチチャンネルオーディオの定位情報に透かしデータを埋め込む方法である。例えば、２チャンネルステレオの場合では音源定位は左右の音圧により決まるが、この音圧バランスを変えることによってデータを埋め込むことができる。ステレオでは平均すると音源定位はスピーカーの中央にあるが、瞬時瞬時では定位は右にずれたり左にずれたりする。この方法ではオリジナルの信号の定位と比較して定位を左右にずらしてデータの「０、１」を表現しており、埋め込んだ透かしデータを取り出すためには、オリジナル信号が必要である。しかし、こ

の方法は、秘密情報を分散して共有するという秘密情報分散手法ではなく、埋め込み方法が分かってしまうと、埋め込まれた電子透かし情報が破壊されてしまうという欠点がある。

【０００３】

【非特許文献１】

シャミア著（Adi Shamir, "How to share a secret," Communications of the ACM, Vol.22,No.11,pp.612-613,1979）

【非特許文献２】

スタドラー著（ Markus Stadler, "Publicly Verifiable Secret Sharing," EUROCRYPT'96, Lecture Notes in Computer Science 1070,pp.190-199,1996）

【非特許文献３】

オガタ著（ Wakaha Ogata, "On the Practical Secret Sharing Scheme," IEICE Trans. Fundamentals, Vol.E84-A,No.1,pp.256-261, 1999）

【非特許文献４】

ナオア他著（Moni Naor, Adi Shamir, "Visual Cryptography," EUROCRYPT'94, Lecture Notes in Computer Science 950, pp.1-12,1994）

【非特許文献５】

コガ著（Hiroki Koga "A General Formula of the (t,n)Threshold Visual Secret Sharing Scheme," ASIACRYPT2002, Lecture Notes in Computer Science 2510, pp.328-345,2002）

【非特許文献６】

デスメット他著、「非バイナリ音声暗号化」（Yvo Desmedt,Tri Van Le, Jean-Jacques Quisquater, "Nonbinary Audio Cryptography," Information Hiding'99, Lecture Notes in Computer Science 1768,pp.478-489,1999）

【非特許文献７】

富岡淳樹、中村高雄、小川宏、高嶋洋一著、「マルチチャンネルディジタルオーディオに対する電子透かし」（1998年、（社）電子情報通信学会発行）

【０００４】

【発明が解決しようとする課題】

上述したように従来の音響秘密分散手法では、音信号に複雑な処理が必要であるためコストがかかり不便であった。そこで、本発明は、複雑な信号処理を必要としない、音像定位を活用した音響秘密分散技法を提供することを目的とする。

【０００５】

【課題を解決するための手段】

本発明による音響秘密情報分散装置は、音像定位を活用した音響秘密情報分散装置であって、

秘密情報として少なくとも１つのターゲット音を複数のステレオメディアに分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央からずれるように分散する第1の信号処理器と、

攪乱情報として複数のデコイ音を前記複数のステレオメディアにそれぞれ分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央に定位するように分散する第２の信号処理器と、

を含むことを特徴とする。

本発明によれば、音像を頭部中央からずれるか否かという簡易な処理で秘密情報を分散でき、人間の聴覚特性を使った秘密情報の復号が可能となる。即ち、本発明によれば、分散情報の生成、および、秘密情報の復元の両方において、信号処理を極力減らすことが可能となる。こうして作成された複数のステレオメディアを別々に格納しておけば、結託に極めて強い安全な秘密情報の分散が可能となる。

【０００６】

また、本発明による音響秘密情報分散装置は、

前記第1の信号処理器および前記第2の信号処理器は、

前記ステレオメディアの左右のチャンネルの音量を調整することによって、前記音像が頭部中央からずれるか否かを制御している、

ことを特徴とする。

本発明によれば、左右のチャンネルの音量を調整するという非常に簡易な処理で音像を頭部中央からずれるか否かという処理が可能となる。

【０００７】

また、本発明による音響秘密情報分散装置は、

所望の安全率（前記ターゲット音か前記デコイ音かを特定され得る分散配置となる上界値）、および／または、想定される結託者率に基づき、所定の計算式を用いて前記ステレオメディア数を算出する計算手段と、

（オプション）前記計算手段で算出された前記ステレオメディア数を用いて分散するよう前記第1の信号処理器および前記第2の信号処理器を制御する制御手段と、

をも含むことを特徴とする。

本発明によれば、ユーザが許容可能な安全率や予想される結託者率を入力することによって、これら条件を満足させるメディア数が容易に設定可能となる。従って、所望の安全率を簡易かつ確実に保障することが可能となる。

【０００８】

また、本発明は上述した各装置に対応する方法、プログラムとしても実現可能である。

例えば、本発明による音響秘密情報分散方法は、音像定位を活用した音響秘密情報分散方法であって、

秘密情報として少なくとも１つのターゲット音を複数のステレオメディアに分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央からずれるように分散する第1のステップと、

攪乱情報として複数のデコイ音を前記複数のステレオメディアにそれぞれ分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央に定位するように分散する第２のステップと、

を含むことを特徴とする。

【０００９】

また、本発明による音響秘密情報分散方法は、

前記第1および前記第2のステップは、

前記ステレオメディアの左右のチャンネルの音量を調整することによって、前記音像が頭部中央からずれるか否かを制御している、

ことを特徴とする。

【００１０】

また、本発明による音響秘密情報分散方法は、

所望の安全率、および／または、想定される結託者率に基づき、演算手段を用いて前記ステレオメディア数を算出する計算ステップ、

をも含むことを特徴とする。

【００１１】

また、本発明によるプログラムは、音像定位を活用した音響秘密情報分散方法をコンピュータに実行させるためのプログラムであって、

前記方法は、

秘密情報として少なくとも１つのターゲット音を複数のステレオメディアに分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央からずれるように分散する第1のステップと、

攪乱情報として複数のデコイ音を前記複数のステレオメディアにそれぞれ分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央に定位するように分散する第２のステップとを含む

ことを特徴とする。

【００１２】

また、本発明によるプログラムは、

前記第1および前記第2のステップは、

前記ステレオメディアの左右のチャンネルの音量を調整することによって、前記音像が頭部中央からずれるか否かを制御している、

ことを特徴とする。

また、本発明によるプログラムは、

所望の安全率、および／または、想定される結託者率に基づき、演算手段を用いて前記ステレオメディア数を算出する計算ステップ、

をも含むことを特徴とする。

【００１３】

また、本発明による装置、方法、およびプログラムにおいては、

前記ターゲット音の数と前記デコイ音の数との和ｎ（即ち音信号の種類）は、６

以下とする、
或いは、前記ステレオメディアにおける１つの音信号の片側の最大振幅ｐは、ほぼ１０以下とする、
ことが好適である。

【００１４】

【発明の実施の形態】

以下、諸図面を参照しつつ本発明の原理および実施態様を詳細に説明する。

図１は、本発明による音響秘密情報分散装置の構成の一例を示すブロック図である。図に示すように、本発明による音響秘密情報分散装置１００は、第1の信号処理器１１０、第２の信号処理器１２０、格納手段１３０および送受信手段１４０を具える。第1の信号処理器１１０は、秘密情報として少なくとも１つのターゲット音を複数のステレオメディアに分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央からずれるように分散する。第２の信号処理器１２０は、攪乱情報として複数のデコイ音を前記複数のステレオメディアにそれぞれ分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央に定位するように分散する。こうして作成された複数のステレオメディアは一旦、ハードディスクなどの格納手段（装置）１３０に格納される。その後、ステレオメディア（即ち音声ファイルであり、送信前に圧縮することが好適である）は送受信手段１４０によってネットワーク２００を介して、メディアと同数である複数の分散場所３００に存在するＰＣ、サーバなどへ送信され別々に保管されることとなる。送信が終了した後で格納手段（装置）１３０の情報は削除される。秘密情報を復元したい場合は、複数の分散場所（被分配者）３００にあるＰＣなどにメディアを送信するよう促し、全てのステレオメディアを受信して、これらメディアを同時に再生して、人間が聴取すれば、「音像のずれ」によって秘密情報である「少なくとも１つのターゲット音」を識別することができる。また、本装置１００は、後述する分散アルゴリズムによる処理を各信号処理器に実行させるための制御信号などを算出するＣＰＵ（図示しない）、所望の安全率および／または想定される結託者率に基づきステレオメディア数を算出する計算手段（図示しない）

、および前記計算手段で算出された前記ステレオメディア数を用いて分散するよう前記第1の信号処理器および前記第2の信号処理器を制御する制御手段（図示しない）を具える。

【００１５】

なお、秘密情報としてのターゲット音は、好適には１つであるが、例えば、右側に聞こえるターゲット音を１つ、左側に聞こえるターゲット音を１つという形式で複数の音を秘密情報とすることも可能である。また、本発明においては、ターゲット音は、他のデコイ音と区別さえできればよいため、例えば、ターゲット音の音像を右側に定位させ、デコイ音を全て左側に定位するという構成や、ターゲット音の音像のみを中央に定位させ、他のデコイ音を左右に定位させるという構成なども取り得る。

【００１６】

方向知覚

本発明は人間の「方向知覚」の特性を利用している。人間は目をつぶっても、音がどちらかから聞こえてくるかを容易に判断することができる。壁や物のために反射音が多いなどの特殊な音響条件でない限り、日常の経験では音の方向を間違えることはほとんどない。こうした音源の方向の知覚は、主に左右の耳に到着する音波のわずかな時間の違いと強さの違いを手がかりにして行なわれている（「日本音響学会、境久雄、中山剛著、「聴覚と音響心理」，コロナ社，1978」を参照されたい。）。従って、バイノーラル（binaural）聴覚と呼ばれるヘッドホンを用いた聴取により左右の音の時間の差をなくすことで、人間の聴覚は左右の音量の差だけで方向知覚を行うことになる。バイノーラル聴取では音が左右から同じ音量で聞こえると、その音の音像は頭部中央に定位し、左右のどちらかの音量が大きいと、音像は頭部中央より音量が大きい側に傾くことが知られている。また、中央から音像が傾く閾値は、左右の音圧レベル（ＳＰＬ）差が約１dB程度のときであり、２dB以上の音圧レベル差があれば、人間は無理なく容易に音像の傾きを認識できるとされている。

【００１７】

本発明では、音像を頭部中央からずらすことを制御するが、これには各種の方

法が考えられるが、その制御方法の１つとして逆位相の音を用いる場合を説明する。その性質は以下のとおりである。

性質１（逆位相の音）

・モノラル、またはステレオの同じチャンネルで、正位相の音とその位相の音を重ねあわせると無音になる。

・一方の側に正位相の音、もう一方の側に逆位相の音を記録したステレオメディアを聴くと、元の音とは異なるぼやけた音となる。

・モノラルとステレオのいずれにおいても、正位相の音を聴いても、逆位相の音を聴いても全く同じ音に聞こえる。

【００１８】

本発明は、「複数存在する音信号の中のどの音信号がターゲット音であるか？」という情報を秘密情報とする音響秘密分散手法である。具体的には、1つのターゲット音をn－１個の攪乱用のデコイ音に紛れ込ませてｋ枚のメディアに分散配置し、このｋ枚のメディアを同時再生することで、n個の音信号のうちの1つのターゲット音を特定する。音信号自体に秘話性を持たせるわけでないないため、それぞれの音信号がありのままに聞こえても問題ない。

聴覚特性の方向知覚を利用することにより、ｋ枚の分散メディアを合わせたときに、n－１個のデコイ音を頭部中央に定位させ、ターゲット音を頭部中央より左右どちらかに傾かせるように分散メディアをつくることで、「どの音がダーゲット音であるか？」という秘密を特定できる。この方法を用いれば、分散情報の作成にかかる手間は、それぞれの音信号の左右の音量を設定するという非常に簡易かつ簡便な処理で済み非常に有効である。

また、左右の音量差を変えることで、音信号の頭部内での定位する位置が決定されるので、分散メディアとして左右に記録することができるステレオのメディアを用いる。

【００１９】

音信号ごとの分散規則

ｎ種類の音信号の内の、ある1つの音信号をNo.1～No.５の5枚のステレオメディアに分散した例を表１に示す。

【００２０】

【表１】

	L	R
Ｎｏ.１	５	－２
Ｎｏ.２	－４	－６
Ｎｏ.３	－２	１０
Ｎｏ.４	８	－３
Ｎｏ.５	－７	－２
合計	０	１

【００２１】

この表１で＋１は正位相、－は逆位相を表し、数字は音信号を重ね合わせた回数（振幅、または音量）を表している。また、Ｌはステレオ音の左側、Ｒはステレオ音の右側を表している。この例ではＮｏ.3のメディアの左側に音信号の左の音の位相を反転し2回重ね合わせたものを記録している。また５枚のメディアに記録されている音信号の合計をとると左側が０で無音になり、右側は＋１で音信号が聞こえる。従ってこの音信号は、頭部中央に定位しないためターゲット音である。

【００２２】

ターゲット音の生成規則

ひとつの音信号を、表2のようにｋ枚のメディアに配置させたとする。

【表２】

	L	R
Ｎｏ.１	ℓ_1	r_1
Ｎｏ.２	ℓ_2	r_2
・ ・	・ ・	・ ・
Ｎｏ.ｋ－１	ℓ_{k-1}	r_{k-1}
Ｎｏ.ｋ	ℓ_k	r_K

この音信号がターゲット音になるには、

【数１】

$$(\sum_{i=1}^{k}\ell_i,\sum_{i=1}^{k}r_i)=(0,1)or(1,0)or(0,-1)or(-1,0) \qquad (1)$$

を満たさなければならない。

【００２３】

デコイ音の生成規則

同様の状況で、この音信号がデコイ音になるには、

【数２】

$$(\sum_{i=1}^{k}\ell_i,\sum_{i=1}^{k}r_i)=(0,0)or(1,1)or(-1,-1) \qquad (2)$$

を満たさなければならない。デコイ音の生成規則では、（＋１，－１）、（－１，＋１）を採用しない。このように左右の振幅が同じであるにも関らず位相が反転している音をバイノーラル聞き取りすると、頭部内で音像が定位せず、ぼやけた音になるからである。ターゲット音とデコイ音との生成規則より、ｋ枚のメディアを同時再生したときに左右のどちらも振幅は０か1になる必要があることが分かる。一方、どの音信号に対しても、１つのメディアに記録できる左右の振幅に上限を設ける。この上限を左右共にｐ＞０とすると、ｌ ｉ とｒ ｉ は、

【数３】

$$\forall i \quad s.t.1\le i\le k,|\ell i|\le p,|ri|\le p \qquad (3)$$

を満たさなければならない。これは、同時再生したときに聞こえる振幅１の音が相対的に小さくなり過ぎることを防ぐためである。

【００２４】

分散配置アルゴリズム

上述した条件を満たす分散配置アルゴリズムを示す。

このアルゴリズムの動作の概要は次のようになっている。まずｉ番目のメディアの左右の値l_i，r_iを選ぶために集合P_l，P_r準備する。このP_l，P_rはｉを$1<i<k-1$の範囲で増加させるにつれて次のように毎回更新される。

このP_l，P_rの要素は、絶対値がｐ以下であり、かつｉ番目のP_l，P_rは$Suml=l_1+\cdots l_{i-1}$，$Sumr=r_1+\cdots r_{i-1}$により求められるSuml、Sumrによって決定され、Suml、Sumrにl_i，r_iをそれぞれ足した値の絶対値も上限ｐを超えないように制限が設けられている。

次に、このように準備されたこのP_l，P_rよりl_i，r_iをそれぞれ一様かつランダムに選ぶ。この処理がP_l，P_rの更新と共に$1<i<k-1$を満たす全てのｉについて実行される。

最後に、$i=k$のとき、（1）式または（2）式、及び（3）式を同時に満たすl_k，r_kが存在するように、上述のP_l，P_rの更新が行われている。

このアルゴリズムは音信号1つに対するものであり、実際にはこのアルゴリムを音信号の種類ｎだけ繰り返すことで秘密情報を分散することができる。

【００２５】

各信号に対する分散配置アルゴリズム

1　Input（p，k）
2　Suml＝Sumr＝0；
3　For（i＝1,...，k－1）
4　P_l＝｛x｜｜Suml＋x｜＜pかつ｜x｜＜p｝
5　P_r＝｛x｜｜Sumr＋x｜＜pかつ｜x｜＜p｝
6　$\ell_i \xleftarrow{R} P_\ell$；$r_i \xleftarrow{R} P_r$
7　Suml←Sumr＋l i；Sumr←Suml＋r i；
8　End　For
9　If　（この音信号がターゲット音）
10　Then（1）式を満たすようにl_k，r_kを決定する
11　Else（2）式をみたすようにl_k，r_kを決定する
12　End　If
13　Output（l_1,....l_k,r_1...　r_k）

【００２６】

もし、Suml＝a＞0とすると、Step４においてP_l＝｛－p，・・・p－a｝となり、このときl_iはStep6において要素数が2p＋1－aである集合P_lからランダムに1つ選ばれることになる。

以後では、l_k，r_kが記録されるメディアＮｏ．ｋに該当する利用者を「最終被配分者」と呼ぶ。

【００２７】

秘密情報の復元

上述した分散配置アルゴリズムを用いれば、任意のl_1，・・・，l_{k-1}，r_1，・・・，r_{k-1}に対して（1）式（2）式を満たすl_k，r_kが存在し、l_k，r_kの設定の仕方によって、音信号をターゲット音にもデコイ音にもできる、なぜなら、アルゴリズムにより、

【数４】

$$|\sum_{i=1}^{k-1}\ell_i| \leq p, |\sum_{i=1}^{k-1}r_i| =\leq p$$

また

$$|\ell_k| \leq p, |r_k| \leq p$$

メディアの左側に関して、

$\sum_{i=1}^{k}\ell_1 = \pm p$のとき、$\sum_{i=1}^{k}\ell_i$は０または±１のどちらかになる（復号同順）

$\sum_{i=1}^{k}\ell_1 \neq \pm p$のとき、$\sum_{i=1}^{k}\ell_i$は、0，1－1のいずかになる。

このことは、メディアの右側についても同様である。従って（１）式を満たすｌｋ，ｒｋも（2）式も満たすｌｋ，ｒｋも必ず存在するからである。

よって、ｎ種類の音信号のうち1つをターゲット音としてこのアルゴリズムを適用することで秘密を分散した値で記録されるため、単に各メディアを個別に再生すると、音量の異なる複数の音が同時に再生されることとなる。

【００２８】

安全性

本発明が提案する手法の安全性を議論するため、まず利用者の能力と安全性について定義する。

定義１（利用者について）

利用者の能力を次のように定める。

・１枚以上のメディアを同時に再生して聞くことができる。

・メディアをコンピュータで解析したり増幅したりすることもできる。

・新しいメディアを作成し、それを分散メディアとして提示することはできない。

・上限ｐ、全メディアの枚数ｋ、音信号の種類ｎの値を知っている。

・メディアに記録されている各音信号の左右の重ね合わされた数を解析で求めることができる。

・結託による攻撃は解析によってわかった重ね合わされた数をもとにターゲット音かデコイ音かを特定しようとすることのみとする。

【００２９】

次に実際に複数の利用者が結託して不正を行う場合を考える。それぞれのメディアには複数の音信号が記録されているが、定義１より不正者は重ね合わされている複数の音信号を分離して、各音信号を重ね合わせた回数を特定できる。実際にはこの処理に手間が掛かり、重ねあわせた回数を必ずしも特定できないことも考えられるため、不正者にとって有利な条件を想定していることになる。

本発明による秘密分散手法の安全性は、上述したアルゴリズムにより分散される個々の音信号がターゲット音かデコイ音かを特定されなければ保障される。従って、ある1つの音信号について考える。

【００３０】

<u>最終被分配者を含まない結託</u>

最終被分配者以外のk－1人の利用者が結託しても、

【数５】

$$|\sum_{i=1}^{k-1}\ell_i| \leq p, |\sum_{i=1}^{k-1}r_i| =\leq p$$

であることにより、最終被分配者のメディアによってターゲット音にもデコイ音にもなれるので、結託者がこの音信号をターゲット音がデコイ音か特定することはできない。従って、最終被分配者が信頼できるならば、本発明による技法で結託が起きてもターゲット音とデコイ音の区別に関する情報が漏れることはない。

【００３１】

<u>最終被分配者を含む結託</u>

最終被分配者を含まない結託とは異なり、最終被分配者を含む結託では、結託に参加しない利用者の所有情報によっては、結託者の解析対象の音信号がターゲット音にもデコイ音にもなりえるという性質を保障できない場合が発生する。このことを確かめるために次の補題を示す。

補題１

結託により音信号がターゲット音かデコイ音かを特定されるのは、不正に参加しない利用者のメディアが全て同一であり、かつ左右の重ね合わせた回数の絶対地（振幅）が必ず上限ｐになる場合である。

証明

前述のように、最終被分配者を含まない結託では、ターゲット音かデコイ音かを特定されることはない。そこで、最終被分配者を含むｋ－ｍ人の結託を考える。結託しない利用者の数はｍであり、そのｍ人の分散メディアの番号をNo.j_1，・・・No.j_mとする。

【数６】

$j_U \in \{j_i, \cdots, j_m\}$とおくと、(3) 式より、

$$|\sum_{u=1}^{m} \ell_{ju}| \leq mp, |\sum_{u=1}^{m} r_{ju}| =\leq mp$$

が成り立っている。ここで、結託者は

$\sum_{i=1, i\neq ju}^{k} \ell_i$ の値を知っているので、 $\sum_{i=1, i\neq ju}^{k} \ell_i$ の値に対する $\sum_{i=1}^{k} \ell_i$ のとり得る値を考える

と表3のように分類することができることが分かる。ｒ$_i$についても同様の関係が成り立つ。

【００３２】

【表３】

$\sum_{i=1}^{k}\ell_i$のとり得る値

$\sum_{i=1,i\neq ju}^{k}\ell_i$	$\sum_{i=1}^{k}\ell_i$のとり得る値
ｍｐ＋1	＋1
ｍｐ	0，＋1
ｍｐ－1 ・ ・ －ｍｐ＋1	－1，0，＋1
－ｍｐ	－1，0
－ｍｐ－1	－1

【００３３】

【外１】

$$\left(\sum_{i=1}^{k}\ell_i,\sum_{i=1}^{k}r_i\right)$$

は（1）式（2）式より

（0，±1），（±1，0），（0，0），（±1，±1），

のいずかのみの値を取る。このため結託者が持ち寄った分散情報から求められる

【外２】

$$\left(\sum_{i=1,i\neq j_u}^{k}\ell_i,\sum_{i=1,i\neq j_u}^{k}r_i\right)$$

を用いてターゲット音がデコイ音かを特定できる場合が存在し、このような場合は表４に示す６通りのみとなる。

【表４】

結託に弱い組み合わせ

$\sum_{i=1,i\neq ju}^{k}\ell_i,\ \sum_{i=1,i\neq ju}^{k}r_i$	$\left(\sum_{i=1}^{k}\ell_i,\sum_{i=1}^{k}r_i\right)$	$(\ell_{j_u},\ r_{j_u})$
－ｍｐ，ｍｐ+1	(0, +1)	(+ｐ,－ｐ)
ｍｐ＋１，－ｍｐ	(+1, 0)	(－ｐ，＋ｐ)
ｍｐ，－ｍｐ－１	(0，－1)	(－ｐ，＋ｐ)
－ｍｐ－１，ｍｐ	(－１，0)	(+ｐ,－ｐ)
ｍｐ+1，ｍｐ+1	(+1，+1)	(－ｐ,－ｐ)
－ｍｐ－1，－ｍｐ－１	(－1，－1)	(+ｐ,+ｐ)

従って、ターゲット音かデコイ音かを特定される場合では、不正に参加しない利用者ｍ人のメディアは全て同一となり、

【数７】

$$(\ell_{j_1},\ r_{j_1}) =\cdots\cdots=(\ell_{j_m},\ r_{j_m})$$

$$= (+p,\ +p)\ \mathrm{or}\ (-p,\ -p)\ \mathrm{or}\ (+p,\ -p)\ \mathrm{or}\ (-p,\ +p)$$

のいずれかとなる。上の式を満たしても、表４の組み合わせに該当しなければ特定されることはない。

【００３４】

しかし、ｍ人が同一で結託に弱いメディアを保持している場合、そのほかのk-ｍ人の結託でターゲット音がデコイ音か特定されてしまう場合がある。

例１「ｋ-2人の結託でターゲット音が特定されるとき」

具体的にターゲット音が特定されてしまう場合の例として表４の上から２番目を考える。このとき、

【数８】

$$(\sum_{i=1,i\neq j_u}^{k}\ell_i,\sum_{i=1,i\neq j_u}^{k}r_i)=(+1,0)$$
$$(\ell_{j_1},r_{j_1})=(\ell_{j_2},r_{j_2})=(-p,+p).$$

となっている。この例はNo. ｊ1,No. ｊ2のメディアを保持する２人以外のｋ－2が結託した場合を考えている。まず、結託者は所有する分散情報の和を求め、

【数９】

$$\sum_{i=1,i\neq j_u}^{k}\ell_i=1+2p$$
$$\sum_{i=1,i\neq j_u}^{k}r_i=-2p$$

を得る。これらの値と表３の関係より、取り得る値は、

【数１０】

$$\sum_{i=1}^{k}\ell_i=+1,\sum_{i=1}^{k}r_i=0,-1$$

であることが分かる。次に、この左右の取り得る値と（１）式、（２）式より、結託者は、

【数１１】

$$(\sum_{i=1,i\neq j_u}^{k}\ell_i,\sum_{i=1,i\neq j_u}^{k}r_i)=(+1,0)$$

であることを突き止め、この音信号をターゲット音であると特定する。

【００３５】

<u>定理１</u>

上述した分散配置アルゴリズムを用いて音響秘密分散を行うとき、結託人数をｑとすると、

【数１２】

(i)　　$q \leq k/2-1$

のとき、いずれの音信号についても、結託者はターゲット音かデコイ音かを特定できない。

【数１３】

(ii)　　$k/2-1<q \leq k-1$

のとき、音信号をｎ種類のうち、いずれの音信号についても、結託者がターゲット音かデコイ音かを特定できない確率ｐ１は、

【数１４】

$$P_1 > 1-\sum_{i=k-q}^{k/2} B(i;k,1/p^2)$$

を満たす。但し、B(i;k, 1/p^2)は密度関数

【数１５】

$${}_kC_i(\frac{1}{p^2})^i(1-\frac{1}{p^2})^{k-i}$$

の二項分布を表す。

【００３６】

証明

結託によってターゲット音かデコイ音かを特定されてしまうときに必ず存在する

【数１６】

$$|\ell_i| = |r_i| = p$$

を満たす４種類のメディア(+p, +p)，(-p, -p)，(+p, -p)，(-p, +p)を結託に弱いメディア（l_W, r_W）と呼ぶことにする。この弱いメディア（l_W, r_W）が最も多く存在するのは、

【数１７】

$$(\ell_i, r_i)\begin{cases}(\ell_w, r_w) & i\text{が奇数}\\(-\ell_w, -r_w) & i\text{が偶数}\end{cases}$$

のときであるので、（l_W, r_W）の最大枚数はｋ／２となる。

【数１８】

$$(i) \quad q \le k/2-1$$

のとき、補題１より、結託に弱いメディアがm枚あると、ｋ-m人の結託によってその音がターゲット音かデコイ音かを特定できる場合が存在するが、結託者数がk/2-1人以下では特定されることはない。

【００３７】

【数１９】

$$(ii) \quad k/2-1 \le q \le k-1$$

のとき、No. jのメディアが（l_W, r_W）になる確率を求める。一般性を失わずに、

l_iについて考えると上述した事項から、l_iはp_1からランダムに選ばれているので、Suml＝l_1＋・・・l_{i-1}＝aとすると、

【数２０】

$$\Pr[|\ell_i| = p] = \begin{cases} \dfrac{1}{2p-a+1} < \dfrac{1}{p} & (a \neq 0) \\ \dfrac{2}{2p+1} < \dfrac{1}{p} & (a = 0). \end{cases}$$

同様の関係は、r_jについても導ける。このように左右の両方において独立に1／pより小さくなるので、j番目のメディアが（l_W, r_W）になる確率は、

【数２１】

$$\Pr[|\ell_j| = |r_j| = p] < \frac{1}{p^2}$$

である。従って、メディアk枚のうち、（l_W, r_W）がちょうどI枚だけ存在する確率は高々、

【数２２】

$${}_kC_I\left(\frac{1}{p^2}\right)^I\left(1-\frac{1}{p^2}\right)^{k-I} = B(I;k,1/p^2).$$

である。

【００３８】

これより、ある１つの音信号について、結託者がターゲット音かデコイ音かを特定できない分散配置となる確率p_1は、

【数２３】

$$P_1 > 1 - \sum_{i=k-q}^{k/2} B(i;k,1/p^2)$$

を満たす。ステレオメディア（２チャンネル）に限らずに、dチャンネルのメディアでこのような秘密分散したとき、q人の結託によってターゲット音かデコイ音かを特定されてしまう確率は、

【数２４】

$$\sum_{i=k-q}^{k/2} B(i;k,c/p^d)$$

と予想できる。ここでkは被分配者数、cは定数、pは上限、dはチャンネル数である。

【００３９】

次に各パラメータの設定手法を説明する。

nの設定

nは音信号の種類である。本発明では、「n種類の音信号のうちの唯一のターゲット音はどれか」ということが秘密情報であるため、秘密情報はlog”n”ビットである。従って、nが大きい方が秘密情報の量を増やせるため望ましい。しかし、本発明では、データ復元の際に全メディアを同時再生するため、ターゲット音と同時に聞こえるデコイ音も増えるため、聴覚でのターゲット音の定位が判別不可能になる恐れがある。実際には、頭部中央から傾いて定位する音は、頭部中央に定位する音より電力が－１０dB以上大きくないと聴き取ることが困難である。これらに基づき本発明における音信号の種類ｎ、即ち、ターゲット音数とデコイ音数の和nの設定を行う。

【００４０】

本発明において、全メディア同時再生時に左右どちらかに定位するターゲット

音の振幅は(1)式より１であるため、その電力も１となる。また、デコイ音は(2)式より無音になるか左右共に振幅が１になるかであるので、最悪の場合となる全ての音信号の振幅が左右共に１である場合を考える。このときに頭部中央に定位する全デコイ音（n-1種類）の電力は2(n-1)になる。従って、全メディア再生時にターゲット音を確実に頭部中央からずらして即ち傾いて定位させるためには、

【数２５】

$$10\log_{10}\frac{1}{2(n-1)} \geq -10$$
$$2(n-1) \leq 10$$
$$n \leq 6$$

としなければならない。nを大きくしても、同時再生で確実にターゲット音を特定するためには、ターゲット音の特定を困難にする恐れのある「中央に定位するデコイ音を同時再生で消去する」ことによって解決できるものと考えられる。そのために、デコイ音の生成規則を

【数２６】

$$(\sum_{i=1}^{k} \ell_i, \sum_{i=1}^{k} r_i) = (0,0)$$

に変えてみる。このように変化させたとしても、前述の分散配置アルゴリズムは１つの音信号あたり１回で必ず終了するので、音信号の種類nだけ繰り返すことで秘密分散することができる。この場合の結託への耐性を考えてみる。

【００４１】

結託に参加しない被分配者をm人とする。但し

【外３】

$$m \leq \frac{k}{2} - 1$$

である。そのm人の分散メディアの番号をNo.j_1,…,No.j_mとし

【外４】

$$j_u \in \{j_i, \ldots, j_m\}$$

とする。このとき

【外５】

$$\sum_{i=1}^{k} \ell_i$$

の取り得る値は、前掲の表の同じであるが、取り得る値が+1または-1しかない

【数２７】

$$\sum_{i=1, I \neq j_u}^{k} \ell_i = mp + 1, -mp - 1$$

のときに結託によってターゲット音が特定されてしまう。従って、
メディアの左右どちらかが上限ｐとなるとき結託に対して弱くなり、ある1枚の
メディアの左右どちらかが上限ｐとなる確率は、

【数２８】

$$\Pr[|\ell_i| = p \quad or \quad |r_i| = p] < \frac{2p-1}{p^2} < \frac{1}{p}$$

になる。そのため、q(=k-m)人の結託でターゲット音が特定されてしまう確率は

、

【数２９】

$$\sum_{i=k-q}^{k/2} B(i;k,1/p)$$

となってしまう。デコイ音を上のような限定した生成規則にしてしまうと音像定位という聴覚特性を生かしていないためステレオのメディアを用いる必要もなく、モノラルでも可能である。確率もdチャンネルに対応した式にd=1（モノラル）を代入した確率になってしまい、ステレオの提案手法と比べるとかなり高い確率になってしまう。

【００４２】

pの設定

pは各メディアにおける、１つの音信号の片側の最大振幅である。また、ｋ枚のメディアを同時再生したときに聞こえる音の振幅は１（単位振幅）である。この最大振幅の音も、単位振幅の音も、人が聞き取りやすくするためには、その音量のレベル差の限界は２０ｄＢ程度である。２０ｄＢとは約１０倍であるので、最大振幅は単位振幅の１０倍以下、すなわちｐ≦１０が望ましい。定理１よりｐが大きいほうが安全、即ち結託に強くなるので、実用的にはｐ＝１０とすることが好適である。

【００４３】

ｋの設定

定理１より１つの音信号がターゲット音かデコイ音かを特定されてしまう確率は二項分布の和

【数３０】

$$\sum_{i=k-q}^{k/2} {}_kC_i\left(\frac{1}{p^2}\right)^i\left(1-\frac{1}{p^2}\right)^{k-i} = \sum_{i=k-q}^{k/2} B\left(i;k,1/p^2\right)$$

になることが分かった。

この二項分布の和を標準正規分布に近似することにより上界をkとqの関数として求める。

補題２（二項分布の和の近似）

【数３１】

ある二項分布$B(X;n,p)$の和$\sum_{X=X_0}^{n} B(X;n,p)$は、この二項分布が正規分布に近似できるくらい$n$が十分大きいならば、

$$\Pr[Z \geq Zo] = \begin{cases} \frac{1}{2} - \Pr[0 \leq Z \leq Z_0] & (X_0 \geq E(X)\text{のとき}) \\ \frac{1}{2} + \Pr[0 \leq Z \leq -Z_0] & (X_0 \geq E(X)\text{のとき}) \end{cases}$$

に近似できる。

ただし、Ｚ，Ｚ０はＸ，Ｘ０に対応する標準正規分布の変数で、それぞれ、

【数３２】

$$Z = \frac{X\text{-}np}{\sqrt{npq}} \quad (q = 1\text{-}p)$$

$$Z_0 = \frac{X_0\text{-}np}{\sqrt{npq}}$$

と表される。また、標準正規分布N(0,1)とは、

【数３３】

$$N(0,1)=\frac{1}{\sqrt{2\pi}}e^{-\frac{z^2}{2}}$$

であるような分布である。

【００４４】

定理２（ターゲット音かデコイ音かを特定される分配配置となる確率の上限）

全メディアの枚数をkとしたとき、q人の結託者によってある１つの音信号がターゲット音かデコイ音であるかを特定される分配配置となる確率の上界εは、

【数３４】

$$\varepsilon=\begin{cases}\frac{1}{2}-\Pr[0\le Z\le Z_0] & \left(k/2-1<q\le\left(1-1/p^2\right)k\text{のとき}\right)\\ \frac{1}{2}-\Pr[0\le Z\le -Z_0] & \left(\left(1-1/p^2\right)k\le q\le k-1\text{のとき}\right)\end{cases}$$

但し、

$$Z_0=\frac{p^2(k-q)-k}{\sqrt{k(p^2-1)}}$$

【００４５】

証明

補題２の二項分布B(X;n,p)を提案方式で求めた二項分布B(I;k,1/p^2)に適用する。そのために変数を[p→1/p^2、q→1－1/p^2、n→k、X_0→k－q、X→i]のように変換する。この変換に伴いZ_0は、

【数３５】

$$Z_0=\frac{(k-q)-k(1/p^2)}{\sqrt{k(1/p^2)(1-1/p^2)}}=\frac{p^2(k-q)-k}{\sqrt{k(p^2-1)}}$$

になる。また、q人の結託者によってターゲット音かデコイ音かを特定されてしまう分散配置となる確率

【外６】

$$\sum_{i=k-q}^{k/2} B(i;k,1/p^2)$$

は、

【数３６】

$$\sum_{i=k-q}^{k/2} B(i;k,1/p^2) < \sum_{i=k-q}^{k} B(i;k,1/p^2) \approx \Pr[X \geq X_0] = \Pr[Z \geq Z_0]$$

となる。従って上限εは、

【数３７】

$$\varepsilon = \Pr[Z \geq Z_0] = \begin{cases} \frac{1}{2} - \Pr\left[0 \leq Z \leq \frac{p^2(k-q)-k}{\sqrt{k(p^2-1)}}\right] & (k/2-1 < q \leq (1-1/p^2)k \text{のとき}) \\ \frac{1}{2} + \Pr\left[0 \leq Z \leq -\frac{p^2(k-q)-k}{\sqrt{k(p^2-1)}}\right] & ((1-1/p^2)k \leq q \leq k-1 \text{のとき}) \end{cases}$$

【００４６】

例２（上界から全メディアの枚数を決定する）

p=10とする。このとき全メディアの枚数kのうち0.975ｋの被分配者が結託しても、ターゲット音かデコイ音かを特定される分散配置となる確率を１０－3以下にしたいとする。このときｋの取り得る値はいくらになるのかを求める。

p=10，ｑ＝0.975ｋとなるので、定理２の上の式より、

【数３８】

$$\frac{1}{2}-\Pr\left[0\le Z\le\frac{p^2(k-q-k)}{\sqrt{k(p^2-1)}}\right]^{\varepsilon\le 10^{-3}}\le 10^{-3}$$

$$\Pr\left[0\le z\le\frac{100(k-0k.975k)-k}{\sqrt{k(100-1)}}\right]\ge\frac{1}{2}-10^{-3}$$

$$\Pr\left[0\le z\le\frac{1.5}{\sqrt{99}}\sqrt{k}\right]\ge 0.499$$

【００４７】

累積標準正規分布表より、原点からZ_0までの面積が０．４９９以上となるようなZ_0を求めると$Z_0\geqq 3.08$となる。従ってkは、

【数３９】

$$\frac{1.5}{\sqrt{99}}=\sqrt{k}\ge 3.08$$

$$k\ge 418$$

となる。各音信号、各メディアにおける音信号の振幅の上限ｐをｐ＝10としたとき、ターゲット音かデコイ音かを特定される分散配置となる確率の上界εと被分配者数k、そして結託者数ｑの３つのパラメータのうち１つを固定したグラフを示す。

【００４８】

図２は、k＝100(p=10)に固定したときの、qとεとの関係を示すグラフである。図に示すように、例えば、結託者率が９０％（即ち100人中結託者が90人）を超える辺りから上界値が急激に上昇していることが分かる。

図３は、k＝1000(p=10)に固定したときの、qとεとの関係示すグラフである。図に示すように、例えば、結託者率が９６％（即ち1000人中結託者が960人）を超える辺りから上界値が急激に上昇していることが分かる。

図４は、図中の上部がq＝100(p=10)に固定したときのkとεの関係、真中がq＝1000(p=10)に固定したときのkとεとの関係、下部がε＝10^{-3}, 10^{-10}に固定したときの、kとq/kとの関係をそれぞれ示すグラフである。これらの図（或いは例２のような計算手法）を使用すれば、想定される結託者率において所望の上界値を得るためには、どれくらいのメディア数（k）に設定すべきかを算出することが可能である。

【００４９】

上述したように、本発明は、既存の音響秘密分散手法とは異なった、復号に人間の聴覚特性を使った新規な秘密分散手法である。この手法を使えば、図２、７、８（特に図４）に示すように、約５０人以上の被分配者数（即ちメディア数）に設定すれば、かなりの安全性を確保できる。さらに、好適には、約１００人以上に設定すれば、さらに結託に対して堅牢な秘密分散を実現できる。

【００５０】

上述したように本発明は、秘密分散を音響を用いて実現する技法であり、複数存在する音源のなかに設定した１つのターゲット音がどの音源であるのかを特定するために必要な情報を秘密情報とし、この秘密情報を分散、保管し、必要に応じて分散した情報を持ち寄ることにより、秘密情報を復元する技法であり、音像定位に関する方向知覚という人間の聴覚特性を活用することにより、分散情報の生成、ならびに、秘密情報の復元の両方において、信号処理を極力減らすことが可能であるという特徴を有する。このように本発明は、人間の聴覚特性を活用しているため、音楽、ラジオ、映画など音を利用する産業での利用が考えられる。

本明細書では、様々な実施態様で本発明の原理を説明してきたが、本発明は上述した実施例に限定されず、当業者であれば開示事項に基づき幾多の変形および修正を施すことが可能であり、これら変形および修正されたものも本発明に含まれることを理解されたい。例えば、当業者であれば、本開示に基づき、本発明を、文献６の「非バイナリ音声暗号化」のような音信号そのものを秘密情報とする

手法と組み合わせることで、さらに安全かつ秘密情報の量が大きい音響秘密分散手法を構成することも可能である。

【図面の簡単な説明】

【図１】　本発明による音響秘密情報分散装置の構成の一例を示すブロック図である。

【図２】　ｋ＝100に固定したときの、ｑとεとの関係を示すグラフである。

【図３】　ｋ＝1000に固定したときの、ｑとεとの関係示すグラフである。

【図４】　ｑ＝100に固定したときの、ｋとεの関係、ｑ＝100に固定したときの、ｋとεとの関係、$\varepsilon = 10^{-3}, 10^{-10}$に固定したときの、ｋとｑ/ｋとの関係をそれぞれ示すグラフである。

【符号の説明】

１００　音響秘密情報分散装置

１１０　第1の信号処理器

１２０　第２の信号処理器

１３０　格納手段

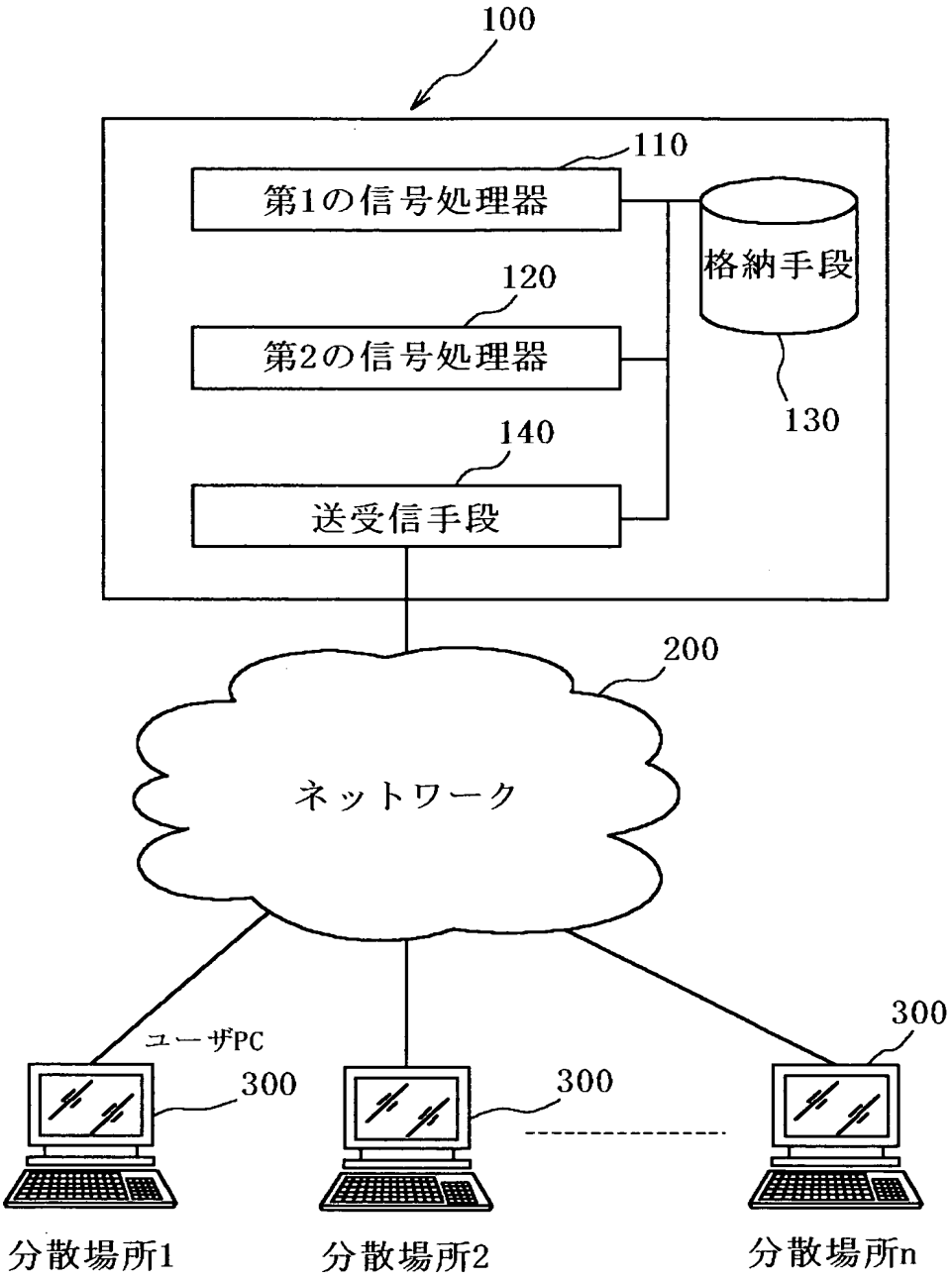
１４０　送受信手段

２００　ネットワーク

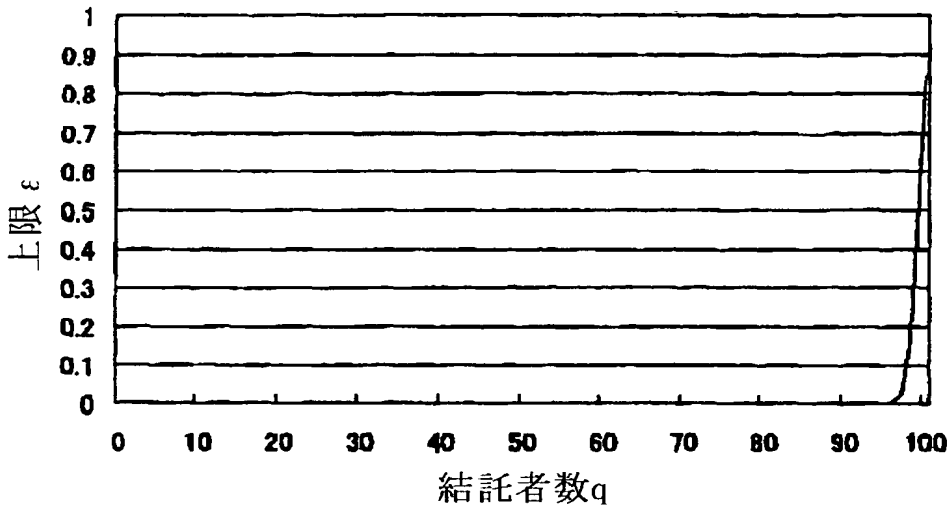
３００　分散場所

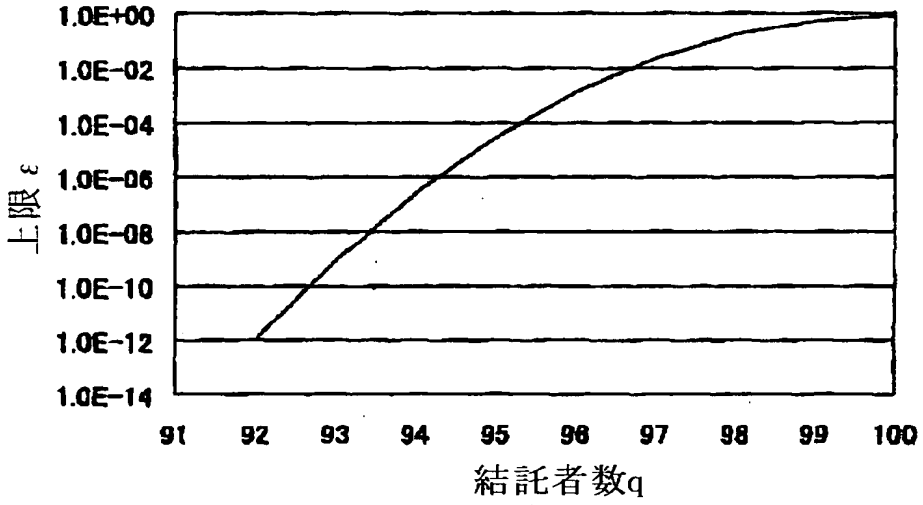
【書類名】　図面

【図１】

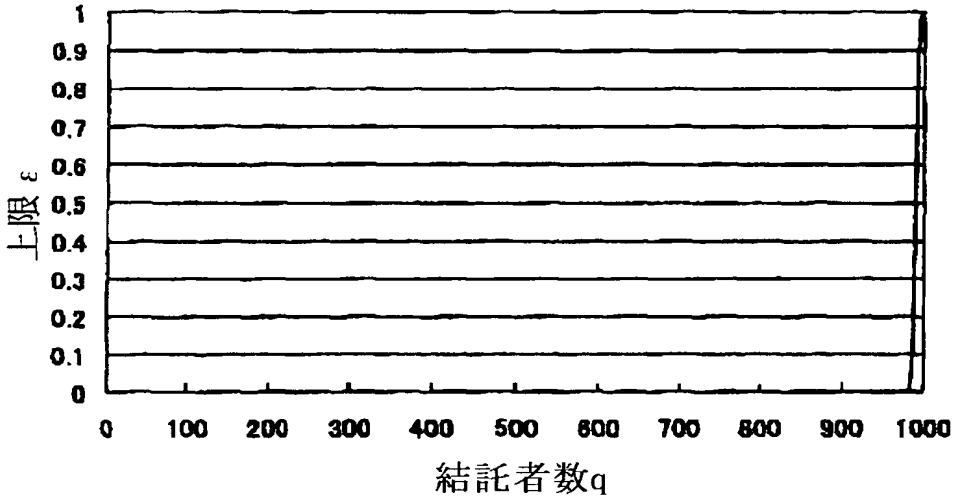

100
110
第1の信号処理器
格納手段
120
第2の信号処理器
130
140
送受信手段
200
ネットワーク
ユーザPC
300
300
300
分散場所1
分散場所2
分散場所n

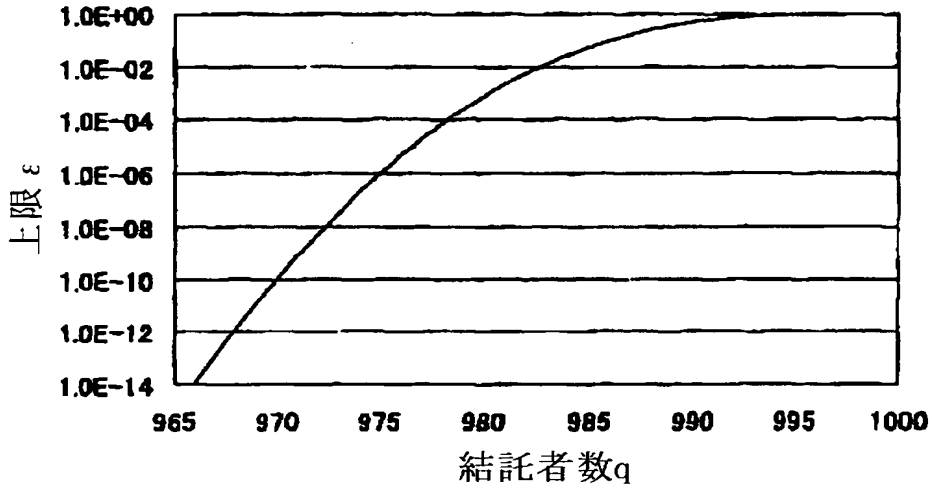
【図２】


1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
上限ε
0
10
20
30
40
50
60
70
80
90
100
結託者数q

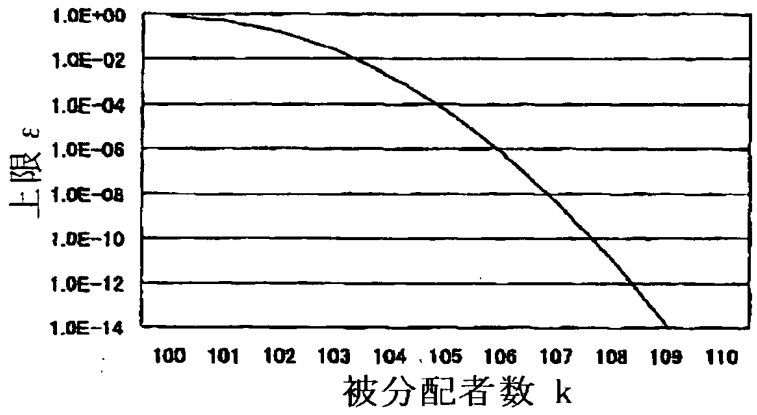

1.0E+00
1.0E-02
1.0E-04
1.0E-06
1.0E-08
1.0E-10
1.0E-12
1.0E-14
上限ε
91
92
93
94
95
96
97
98
99
100
結託者数q

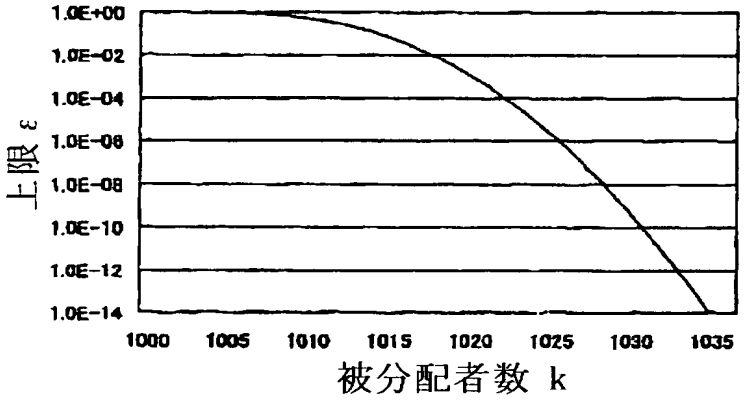
【図３】

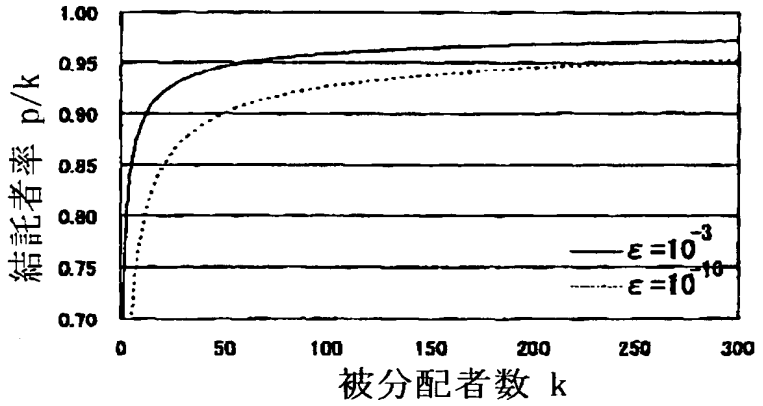

1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
上限ε
0
100
200
300
400
500
600
700
800
900
1000
結託者数q


1.0E+00
1.0E-02
1.0E-04
1.0E-06
1.0E-08
1.0E-10
1.0E-12
1.0E-14
上限ε
965
970
975
980
985
990
995
1000
結託者数q

【図４】


1.0E+00
1.0E-02
1.0E-04
1.0E-06
1.0E-08
1.0E-10
1.0E-12
1.0E-14
上限 ε
100 101 102 103 104 105 106 107 108 109 110
被分配者数 k


1.0E+00
1.0E-02
1.0E-04
1.0E-06
1.0E-08
1.0E-10
1.0E-12
1.0E-14
上限 ε
1000 1005 1010 1015 1020 1025 1030 1035
被分配者数 k


1.00
0.95
0.90
0.85
0.80
0.75
0.70
結託者率 p/k
ε =10^-3
ε =10^-10
0 50 100 150 200 250 300
被分配者数 k

【書類名】　　要約書

【要約】

【課題】　複雑な信号処理を必要としない、音像定位を活用した音響秘密分散技法を提供する。

【解決手段】　音像定位を活用した音響秘密情報分散装置、方法、およびプログラムを提供する。本装置は、秘密情報として少なくとも１つのターゲット音を複数のステレオメディアに分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央からずれるように分散する第1の信号処理器と、攪乱情報として複数のデコイ音を前記複数のステレオメディアにそれぞれ分散し、さらに、これら複数のステレオメディアを同時に再生しバイノーラル聴取する場合に音像が頭部中央に定位するように分散する第1の信号処理器とを含み、再生時の音像のずれによって秘密情報を特定することが可能となる。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００３－２０２００４
受付番号	５０３０１２３６６２８
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　９月　８日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	391012394
【住所又は居所】	宮城県仙台市青葉区片平２丁目１番１号
【氏名又は名称】	東北大学長

【代理人】　申請人

【識別番号】	100072051
【住所又は居所】	東京都千代田区霞が関３－２－４　霞山ビル７階
【氏名又は名称】	杉村　興作

特願２００３－２０２００４

出　願　人　履　歴　情　報

識別番号　　［３９１０１２３９４］

１．変更年月日　　１９９１年　１月２２日
［変更理由］　　新規登録
住　所　　宮城県仙台市青葉区片平２丁目１番１号
氏　名　　東北大学長